

## SECURITY (NEW ENTERPRISE)

---

**Effective Date:** July 1, 2008  
**Revision Date:** April 24, 2008  
**Version:** 1.0.0  
**Product Owner:** Michael Casey  
**Product Manager:** Michael Casey  
**Phone:** 801-538-3470  
**E-mail:** [mcasey@utah.gov](mailto:mcasey@utah.gov)

Enterprise Information Security encompasses the provisioning and management of information security services and solutions to all Executive Branch agencies (defined by § 63F-1-206 of the Utah Technology Governance Act). These services are available to all employees, contractors, partners or vendors who: connect to the State Wide Area Network (WAN), operate or manage telecommunication and information technology services, equipment or data supporting the State's business functions.

### Product Features and Descriptions

Feature	Description
Strategic Planning and Management	Continuously ensure the enterprise's information security program (principles, practices and system design) is in line with all state agency mission statements.
Risk Management	Provide a balanced approach to the identification and assessment of risks to information assets, and the management of mitigation strategies that achieve needed security at an affordable cost.
Information Security Management	The development and management of principles, policies, and procedures necessary to ensure the confidentiality, integrity, availability, and privacy of information in all forms of media (electronic and hardcopy) throughout the information life cycle.
Information Security Training & Awareness	The development and delivery of training and activities designed to instruct workers about their security responsibilities, and the delivery of information security processes and procedures for performing duties optimally and securely within related environments.
Quality Assurance and Compliance	The review, evaluation, analysis of processes against statutory requirements, information security laws, regulations, industry-wide best practices, enterprise security process, procedures, standards, and policies to achieve the State's information security program goals.
Vulnerability Management	The identification and testing of vulnerabilities to information assets, the issuance of recommendation(s), and the management of mitigation strategies that achieve needed security at an affordable cost.

## Product Features and Descriptions

Feature	Description
Incident Management	The development and issuance of processes and procedures to prepare and prevent, detect, contain, eradicate, recover and apply lessons learned from incidents impacting the mission of the State, and its agencies, including investigation and analysis used for recovering, authenticating, and analyzing electronic information to reconstruct events related to security incidents.
Security Operations and Maintenance	The maintenance, monitoring, control, and protection of the infrastructure, and the information residing on it, during the operational phase of information systems and/or applications in production.
Network Security and Telecommunications	Provides security for basic network services and information and provides maintenance for the hardware layer on which it resides.
Enterprise Continuity	Ensures the enterprise continues to perform essential IT business functions after the occurrence of a wide range of potential catastrophic events. Enterprise Continuity relates to IT assets and resources and associated Information security requirements.
System and Application Security	Ensures that the operation of IT systems and software does not present undue risk to the enterprise, and its information assets, through the integration of information security into an IT system or application during the System Development Life Cycle (SDLC).
Procurement	The planning and evaluation of information products or services that are being purchased. The evaluation includes "risk-based" pre-solicitation, solicitation, source selection, award, and monitoring, disposal, and other post-award activities.

## Features Not Included

Feature	Explanation
Physical Security	Protect the agency's personnel, equipment, and information from natural or manmade treats to physical facilities where information equipment is located or work is performed (e.g., computer rooms, work locations).
Personnel Security	Ensure the agency's selection and application of human capital (both employees and contractors) are controlled to promote security.

## Rates and Billing

Feature	Description	Base Rate
Security (New Enterprise) Product Features	All product features described above.	\$8.00/device/month

## Ordering and Provisioning

To obtain information and/or support regarding Enterprise Information Security services, contact the DTS Enterprise Information Security Office (EISO) via the DTS Customer Support Center at (801) 538-3440 or 1-800-678-3440.

## DTS Responsibilities

It is the responsibility of DTS Enterprise Information Security Office to deliver effective enterprise focused security services by:

- Providing support during published hours for questions and/or problems.
- Provide support 24 x 7 in the event of an emergency.
- Maintain applicable vendor contracts for products and services provided.
- Notify customers of any changes to the product prior to changes whenever possible.

## Agency Responsibilities

Ensure that Division/agency employees, contractors, partners and vendors who connect to the State Wide Area Network (WAN), operate or manage telecommunication and information technology services, equipment or data which supports the State's business functions abide by DTS Enterprise Information Security policies, procedures, standards, and guidelines.

Develop and implement division/agency procedures and governance to ensure that incidents are captured and that work is recorded in a timely fashion.

Report suspicious activities associated with automation systems and/or applications to the DTS EISO as soon as possible.

## Service Levels and Metrics

The EISO is accessible 24x7 by telephone at (801) 538-3440 or 1-800-678-3440. Published "Business Hours" for the EISO Service are 7:30 AM-5:30 PM, Monday-Friday. Hours of support/on-call coverage may vary by agency/division/region and product.

EISO staff will exert all reasonable efforts to meet the Time to Initial Response (TIR) and Total Time to Resolution (TTR) targets set forth below.

### Incident Response and Resolution Targets

<b>Time to Initial Response Targets</b>	<b>% Tickets</b>	<b>Total Time to Resolution Targets</b>	<b>% Tickets</b>
Low priority – 2 Business Days	75%	Low priority - 2 Business Days	75%
Medium priority – 1 Business Day	75%	Medium priority - 1 Business Day	75%
High priority – Immediate Response	90%	High priority - 4 Clock hours	75%
Urgent priority – Immediate Response	95%	Urgent priority - 3 Clock hours	100%